Organized financial cybercrime

Leukfeldt, E. R.Rutger; Kruisbergen, E. W.Edwin; Kleemans, E. R.; Roks, R. A.Robert

published in
The Palgrave Handbook of International Cybercrime and Cyberdeviance
2020

DOI (link to publisher)
10.1007/978-3-319-78440-3_65
10.1007/978-3-319-90307-1_65-1

document version
Publisher's PDF, also known as Version of record

Organized Financial Cybercrime: Criminal Cooperation, Logistic Bottlenecks, and Money Flows

E. R. (Rutger) Leukfeldt, E. W. (Edwin) Kruisbergen,
E. R. (Edward) Kleemans, and R. A. (Robert) Roks

Contents

This literature review is based on a Dutch report the authors published in 2018 (Kruisbergen et al. 2018). An English summary is available at: https://english.wodc.nl/.

E. R. R. Leukfeldt (✉)
Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), The Hague University of Applied Sciences, Amsterdam, Netherlands
e-mail: rleukfeldt@nscr.nl

E. W. E. Kruisbergen
Research and Documentation Centre, Dutch Ministry of Justice and Security, The Hague, Netherlands
e-mail: e.w.kruisbergen@minvenj.nl

E. R. E. Kleemans
Vrije Universiteit Amsterdam, Amsterdam, Netherlands
e-mail: e.r.kleemans@vu.nl

R. A. R. Roks
Erasmus University Rotterdam, Rotterdam, Netherlands
e-mail: roks@law.eur.nl

T. Holt, A. M. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, https://doi.org/10.1007/978-3-319-90307-1_65-1

Abstract

This chapter provides an overview of what we know about organized forms of cybercrime executed with a financial goal. First, criminal cooperation is covered. We discuss recent insights into the structure, composition, and mechanisms of origin and growth. Second, bottlenecks in the criminal business process and criminal money flows are described. Every criminal business process entails logistical bottlenecks: logistical problems that must be resolved to ensure the successful execution of criminal activities. One major bottleneck is safely spending illegally obtained money without drawing the attention of the authorities. After all, when it comes to financial cybercrime, the goal of criminals is gaining financial benefits. Finally, in the last section of this chapter, several overarching conclusions about organized forms of cybercrime are presented.

Keywords

Cybercriminal network · Criminal network · Organized crime · Cybercrime · Dark web

Introduction

This chapter examines the collaborations between cybercriminals. A well-known fact in the criminological literature is that most criminals cooperate quite intensively with other criminals (e.g., Shaw and McKay 1931; Sutherland 1937; Reiss 1988; Reiss and Farrington 1991; Andresen and Felson 2010). For the successful commission of crimes, various people with specific human and social capital – knowledge, expertise, and contacts – are often required. The same applies to cybercriminals. Although there are hackers who can hack into systems on their own, studies show that when it comes to financially motivated cybercrimes, various individuals with diverse knowledge and skills are required to commit crimes, including phishing, banking malware, and ransomware (Grabosky 2007; Broadhurst et al. 2014; Hutchings 2014; Leukfeldt 2014, 2016; Leukfeldt et al. 2017a, b, c, d, e, f; Kruisbergen et al. 2018).

Despite the fact that cooperation and social capital still seem to be important for cybercriminal networks, digitization also provides new opportunities for criminal collaboration and changes the ways criminals meet, interact, and execute their crimes. Online meeting places on the clear web and dark web, for example, enable individuals to get in touch with others from all over the world and enter into new criminal collaborations. Knowledge and expertise can be purchased relatively easily on online markets where all sorts of criminal tools and services are offered, including review and rating systems distinguishing reliable from unreliable sellers.

This chapter provides an overview of what we know about organized forms of cybercrime executed with a financial goal. We, therefore, exclude networks having, for example, a solely political or ideological goal. First, criminal cooperation is covered. We discuss recent insights into the structure, composition, and mechanisms of origin and growth. Second, bottlenecks in the criminal business process and criminal money flows are described. Every criminal business process entails logistical bottlenecks: logistical problems that must be resolved to ensure the successful execution of criminal activities. One major bottleneck is safely spending illegally obtained money without drawing the attention of the authorities. After all, when it comes to financial cybercrime, the goal of criminals is gaining financial benefits. Finally, in the last section of this chapter, several overarching conclusions about organized forms of cybercrime are presented.

Criminal Cooperation and the Use of IT

What do we know about the origin of cybercriminal networks? What are the opportunities and limitations for the growth of these criminal networks? In this section, we focus on criminal cooperation and the use of IT by discussing recent insights into the structure, composition, origin, and growth of cybercriminal networks.

Structure and Composition

In theory, the Internet offers a viable opportunity structure for decentralized, flexible networks of criminals who are loosely organized and divide their activities based on knowledge and skills. Various studies show that cybercriminals use online meeting places to meet suitable co-offenders or to buy criminal tools from enables (e.g., Peretti 2008; Lu et al. 2010; Holt and Lampke 2010; Yip et al. 2012; Soudijn and Monsma 2012; Holt 2013; Holt and Smirnova 2014; Decary-Hétu and Dupont 2012; Decary-Hétu et al. 2012; Motoyama et al. 2013; Lusthaus 2012; Dupont et al. 2016). However, this does not mean that all cybercriminal networks are using these online meeting places, and the structure of cybercriminal networks, therefore, is always decentralized and flexible. In practice, this picture seems to be more complex. There are networks that fully use the opportunities of the Internet. For example, members of certain networks can quickly gain an international position through the use of online criminal meeting places (Leukfeldt et al. 2017c, d) or enter into a chain-like collaboration with other criminals who each carry out a specific criminal activity (Bulanova-Hristova et al. 2016; Odinot et al. 2017). The members of these networks only know each other by their online nicknames and recruit specialists on encrypted chat channels and markets on the open and dark web. However, there are also networks at the other end of the spectrum, with a fixed group of core members who have known each other for a long time from the offline world and only use criminal facilitators that can be recruited from their own offline social network.

Empirical research into organized cybercrime in the Netherlands, Germany, England, Sweden, and the United States shows that the structure of a number of cybercriminal networks is similar to that of traditional networks (Bulanova-Hristova et al. 2016; Werner and Korsell 2016; Leukfeldt et al. 2017b, c, d; Odinot et al. 2017; Kruisbergen et al. 2018; Leukfeldt et al. 2019). For example, most of the cybercriminal networks studied by these authors consisted of a more or less stable group of core members who committed offenses together for a prolonged period of time. The core members of these networks often knew each other from the physical world. Only a limited number of specialists were recruited through online meeting places. In addition, only a few networks turned out to be ad hoc collaborations in which alliances were forged at an online meeting place, leading up to attacks being carried out together.

Furthermore, several studies on cybercriminal networks illustrate, similar to traditional networks, the importance of actors functioning as brokers (Soudijn and Monsma 2012; Lu et al. 2010; Yip et al. 2012; Holt and Smirnova 2014; Décary-Hétu and Dupont 2012; Décary-Hétu et al. 2012; Leukfeldt et al. 2017c, e, 2019). Traditionally, so-called brokers were needed to overcome the limitations of offline social networks. In the pre-digital era, only real-world social contacts could be used to get into touch with other criminals and to expand criminal networks (see, e.g., Ianni and Reuss-Ianni 1972; Kleemans and De Poot 2008; Edwards and Levi 2008; Bouchard and Morselli 2014). However, social clusters are always limited, for example, to a region or country. In order to expand the criminal network and the criminal capabilities of the network, contacts have to be forged outside the initial social cluster. Offender convergence settings and brokers can be used to do just that (for more information about offender convergence settings, see the subsection "Forums as Online Meeting Places"). Due to his unique position, the broker is an important node in the criminal network. Even though cybercriminals now are able to use online meeting places to get into touch with other suitable criminals, the overall conclusion from both qualitative analysis of police files and quantitative social network analysis of forum data is that, overall, although in some cases the role of brokers seems to diminish, networks still include members that are more important for the functioning of the network than others (Soudijn and Monsma 2012; Lu et al. 2010; Yip et al. 2012; Holt and Smirnova 2014; Décary-Hétu and Dupont 2012; Décary-Hétu et al. 2012; Leukfeldt et al. 2017c, e).

Finally, there is evidence that cybercriminal networks have a certain degree of hierarchy. Despite the absence of Mafia-like pyramidal organizational structures, all analyzed networks by Leukfeldt et al. (2017a, b, c) have several different and discernible layers of members. Core members are at the top of the network. They work together for a long time, engage in planning criminal activities, and find other suitable co-offenders. Below the core members, there are facilitators providing specific criminal services to improve the criminal activities of the core members of the criminal network. A distinction can be made between professional and recruited facilitators: the former offer their services to all kinds of networks, whereas the latter are recruited by core members to provide specific services for the criminal network. The bottom layer of the network is formed by so-called money mules. This is a group

of criminals who are deployed either by the core members or by facilitators, to shield the criminal activities of the network from law enforcement authorities. For example, the accounts of money mules are used to withdraw the cash of victims of phishing.

In conclusion, there are networks showing many similarities with traditional criminal networks – long-term cooperation between the core members and dependency relationships – and there are networks in which the specialized individual members are engaged in more short-term collaborations. These differences in structure are related to the origin and growth processes of these networks (Bulanova-Hristova et al. 2016; Leukfeldt et al. 2017b, c, d). Traditional criminal networks that also start engaging in cybercrimes retain their original structure. Networks that only commit cybercrimes but are the results of offline social contacts also have a similar structure to that of traditional criminal networks. Networks that only commit cybercrimes and where the core members met each other online sometimes have a traditional structure (contacts on online meeting places can also be long-term; see, e.g., Leukfeldt et al. 2017c, d), but this type of network also sometimes demonstrates short-term (chain-like) cooperation.

Facilitators

Similar to traditional networks, facilitators also play an important role in cybercriminal networks. A few networks manage to commit crimes without the services of others, but the majority of the networks make (extensive) use of facilitators (Odinot et al. 2017; Bulanova-Hristova et al. 2016; Leukfeldt et al. 2017a, b, c, d, e; Kruisbergen et al. 2018; Leukfeldt et al. 2019). Indeed, that is exactly why there is so much activity on online meeting places such as cryptomarkets (e.g., Peretti 2008, Holt and Lampke 2010; Chu et al. 2010; Soudijn and Monsma 2012; Lu et al. 2010; Yip et al. 2013; Holt 2013; Holt and Smirnova 2014). We can distinguish between professional criminal facilitators who offer their services themselves and work for all sorts of criminal networks and recruited criminal facilitators deployed by a specific network. Examples of professional criminal facilitators are malware writers supplying malware that can be used to take over computers, hackers offering their services to break into databases, or people having access to networks of money mules in all sorts of countries that can be used to launder money. These professional criminal facilitators often offer their services on forums, but contacts between core members and facilitators can also be established within offline social networks or offline criminal meeting places. Examples of recruited criminal facilitators are bank employees who provide data of "interesting" bank accounts or who can increase withdrawal and credit limits, which means fewer accounts of money mules are required when "cashing" money originating from phishing attacks. Usually, these facilitators are recruited through offline or online social contacts (see, e.g., Leukfeldt et al. 2017a, b, c, d, e, f).

Little is known about the role that facilitators play in bridging the gap between the "underworld" and "upperworld" for cybercriminal networks. For example, the study of Leukfeldt et al. (2017a) shows that even though respondents indicate that in some

cases there has to be involvement of corrupt Eastern European or Russian government employees, no such evidence was found in the analyzed criminal investigations. It is clear, however, that employees of legitimate companies are sometimes recruited by members of cybercriminal groups to cooperate during criminal activities. This is exemplified by the earlier mentioned bank employees who have insight into the accounts of potential victims or who can increase withdrawal of credit limits of the accounts of money mules (Leukfeldt 2014). Legitimate infrastructures are also abused by criminals to commit their offenses (Odinot et al. 2017; Bijlenga and Kleemans 2018). Hosting providers offering legal services, such as renting out server space, or shady or illegal services, such as bulletproof web hosting, make it very difficult for law enforcement agencies to intervene. Another example consists of online advertising companies showing advertisements on a large number of websites and, specifically, reported cases where advertisements spread malware. Furthermore, legitimate companies such as web shops where items are bought with criminally earned money or parcel deliverers who intercept goods purchased with fraudulent transfers are examples of these intertwining legal and illegal interfaces. Finally, this also relates to financial infrastructures that can be abused, for example, for making mutual payments using e-currencies, such as bitcoins, or the use of exchangers converting e-currencies into euros or US dollars (Odinot et al. 2017; Leukfeldt et al. 2017b, c, d, e).

Finally, there is also the fact that IT is, to a certain extent, neutral and that it is often only when it is actually implemented that it leads to illegal activities. This offers many more opportunities for offenders to cooperate with the legal world, particularly in the "gray zone" between legal and illegal applications of IT. Research by Bijlenga and Kleemans (2018) illustrates that criminals sometimes easily find IT expertise in this "gray zone," because certain tools are sometimes offered entirely legally, via the Internet or via Spyshops (in addition to which extra services are provided to criminal customers). Also when tools are modified (for criminal purposes), experts do not need to know beforehand what the tools will eventually be used for. As a result, business cooperation can easily be established (based on supply and demand) via working relationships or via online or offline meeting places. Criminals can also get straight to the point fairly quickly because at the start of the collaboration, the criminal character does not have to be clearly visible to the person concerned or it can be denied afterward (Bijlenga and Kleemans 2018). In that respect, the neutrality of IT facilitates cooperation.

Forums as Online Meeting Places

Due to the large number of criminal service providers on forums, finding suitable criminal facilitators for cybercriminal networks may be less difficult than for traditional networks (Lusthaus 2012; Yip et al. 2013; Holt and Smirnova 2014; Holt et al. 2015; Dupont et al. 2016; Holt and Lampke 2010, Soudijn and Zegers 2012; Leukfeldt 2014; Franklin et al. 2007; Wehinger 2011). In theory, this makes criminal facilitators easier to replace. Nevertheless, the analyses of Bulanova-Hristova et al.

(2016) and Leukfeldt et al. (2017b, c, d) show that cybercriminal groups sometimes cooperate with the same facilitator for a sustained period of time. On the one hand, forums with their rating and review systems have become quite useful at finding reliable facilitators, but on the other hand, we also know that only a very small proportion of the forums have a very high degree of technical expertise (Holt 2007; Holt et al. 2015) and that review systems do not always work well (Holt et al. 2015; Décary-Hétu and Dupont 2013; Dupont et al. 2016). Therefore, the question remains how easily replaceable these facilitators with a very high degree of technical expertise actually are.

Regarding trust and online meeting places, we know that closed forums require a good reputation for entry. To access the forum, potential members are screened by administrators (or members appointed by the administrator), and new members must provide evidence that they are active in cybercrime (e.g., by providing stolen credit card data or a tutorial) (Soudijn and Zegers 2012; Yip et al. 2013; Lusthaus 2012; Ablon et al. 2014; Holt et al. 2015). Lusthaus (2012) also emphasizes the social mechanisms on a forum. In addition, the reputation of a member can be inferred from a specific status, such as "new member," "seller," or "verified seller." Finally, many forums have a review system; members who have purchased data, tools, or services assess the vendor by means of a written review or a score on a rating scale (Soudijn and Zegers 2012; Herley and Florencio 2009; Wehinger 2011; Yip et al. 2013; Lusthaus 2012; Dupont et al. 2016; Décary-Hétu and Dupont 2012, 2013; Holt 2013; Holt and Smirnova 2014; Holt et al. 2015; Chu et al. 2010; Ablon et al. 2014).

Some forums try to make access (or access to certain parts of the forum) selective, through requirements regarding the status of "applicants," relations they have with existing members, or technical skills (has the applicant additional value for existing members?). An analysis by Dupont et al. (2017) of an exclusive forum shows, however, that eventually, many applicants get access to this "exclusive" forum without having the necessary technical added value. It might very well be the case that the commercial pressure to provide access to as many members as possible (which means: potential clients and co-offenders) is stronger than the wish to remain "exclusive" and "safe." This problem is even stronger regarding the selling of stolen data, credit card credentials, and malware, as these goods and services can be easily resold or even "leaked," which means they may immediately lose their commercial value.

To what extent the trust problem is really solved is an important question that still remains to be answered. How do you know a site can be trusted and is not administered by the police (such as Hansa market, taken over by the Dutch police in 2017) or taken down by the administrators (including taking away all the money and data)? How can buyers and sellers trust each other? And how are goods and services delivered and paid? New technical possibilities provide solutions for certain problems, but some problems may still exist or only take a different shape.

Facilitators active on forums offer their services to multiple individuals and networks (e.g., Peretti 2008; Holt and Lampke 2010; Chu et al. 2010; Soudijn and Monsma 2012; Lu et al. 2010; Yip et al. 2013; Holt 2013; Holt and Smirnova 2014). Potential buyers can contact the seller through various channels, for example, via

private message on the forum or chat channels outside of the forum. Payments can be made with currently used virtual currencies, such as Bitcoin, e-Gold, Liberty Reserve, WebMoney, Yandex, and Western Union (Franklin et al. 2007; Holt and Lampke 2010; Holt and Smirnova 2014; Holt et al. 2015).

Various types of goods are offered through such online forums, such as stolen data, cybercriminal tools and services, as well as more traditional items, such as drugs, medicines, and weapons. Stolen data includes data from credit cards, bank accounts and PayPal accounts, and identity documents (Franklin et al. 2007; Holt and Lampke 2010; Peretti 2008; Holt et al. 2015; Chu et al. 2010; Holt and Smirnova 2014; Wehinger 2011; Soudijn and Zegers 2012; Leukfeldt et al. 2017c, d, e, f). Examples of criminal tools are phishing kits and malware (Holt and Lampke 2010; Herley and Florencio 2009; Soudijn and Zegers 2012; Leukfeldt 2014; Leukfeldt et al. 2017c, d; Holt and Smirnova 2014; Chu et al. 2010) or botnets and DDoS attacks (Franklin et al. 2007; Chu et al. 2010; Décary-Hétu and Dupont 2012). Services that are offered include, for example, "escrow services" through which third parties can safely pay (Lusthaus 2012; Yip et al. 2013; Holt and Smirnova 2014; Holt et al. 2015; Dupont et al. 2016), "exchangers" converting virtual money into real money (Holt and Lampke 2010), "money mules" to "cash" criminal earnings (Soudijn and Zegers 2012; Leukfeldt 2014), other "cash-out services" such as buying goods with stolen credit cards (Franklin et al. 2007; Wehinger 2011), and "bulletproof webhosting" (Franklin et al. 2007).

Leukfeldt (2017) also discusses the functions of these online "offender convergence settings": the market function, the social function, and the learning function. According to these authors, the learning function of online forums turns out to be very important and easily accessible for many users. In contrast to normal convergence settings, the constraints of space and time are absent. Bilateral relationships and conversations can be started immediately; even acquaintances can meet here anonymously (without bystanders noticing this). These convergence settings, therefore, can be primarily characterized as a "free market," but anonymity makes building up trust with strangers more difficult. This might be no problem for small business transactions, such as smaller quantities of drugs, particularly when use can be made of "escrow services," which means that the administrators of the website (or a cooperating third party) function as a go-between for payments and deliveries: the seller receives the payment of the buyer only when the buyer receives the ordered goods. This way, an important logistical problem of buyer and seller is solved: buyer and seller do not have to meet each other in person to hand over drugs and money at the same spot and at the same time (with all the accompanied risks of discovery as well as opportunistic behavior, cheating, violence, and conflicts).

Origin and Growth Mechanisms

Within traditional offline criminal networks, social ties play an important role within the processes of origin and growth (e.g., Ianni and Reuss-Ianni 1972; Kleemans and De Poot 2008; Edwards and Levi 2008; Bouchard and Morselli 2014). Offline social

networks are crucial for the success of criminal networks. The right social capital (knowledge, expertise, contacts) is needed to successfully set up criminal collaborations. However, social contacts also have restrictions because they are limited, for example, to a specific region. Contrary to the offline world, no geographical distances have to be bridged in order to come into contact with other perpetrators online. Therefore, distance, location, and time are in principle no longer limiting factors for criminal cooperation.

Several studies show that digitization, and particularly online criminal meeting places, can influence the origin and growth processes of criminal networks. Soudijn and Zegers (2012) and Yip et al. (2012) show that newcomers on virtual meeting places instantly get in touch with existing forum members and take a more central position relatively quickly. The important role that central actors normally play within networks, therefore, seems to decrease in an online environment.

However, the studies by Leukfeldt (2014), Leukfeldt et al. (2017a, c, d, 2019), Bulanova-Hristova et al. (2016), and Odinot et al. (2017) show that cybercriminal networks use both offline social contacts and virtual meeting places. In networks where offline social contacts form the basis for origin and growth, it can be noticed that family, friends, and acquaintances work together and introduce each other to other people just as within traditional criminal networks. Moreover, it turns out that only one single network completely relies on offline social relationships. Online forums are used by these types of networks to acquire specialist knowledge and skills that are lacking in offline social relations, for example, the purchase of advanced malware that can be used to commit fraud with Internet banking. In networks where online contacts form the basis for the origin and growth of the network, a dichotomy can also be observed. On the one hand, members of these networks got to know each other online, for example, via chat channels, or on forums. On the other hand, a minority of the networks seem to be able to carry out criminal activities with only their online contacts. Within these networks, not only the core members got to know each other online, but all facilitators were also recruited online. In other networks the core members met each other online; they recruited online facilitators but also used offline contacts, for example, to set up a network of money mules.

Online meeting places ensure that the traditional limitations of social networks are lifted. In fact, there is no substantial difference with traditional offline criminal meeting places: once you are inside, you can make contact, and you can meet people who can, for example, provide new markets (see Felson 2003, 2006). Therefore, online meeting places are essentially not new. However, it seems that online meeting places are more accessible than offline criminal meeting places (Leukfeldt et al. 2017c, d). For the curious loner, it is easier to hang around and ask questions on public forums than in a bar full of criminals. Moreover, it is important to note that there is a subculture on these forums in which sharing of information about criminal endeavors is fairly normal (Chu et al. 2010; Holt and Kilger 2008; Holt et al. 2012; Hutchings and Holt 2015; Hutchings 2014; Leukfeldt et al. 2017c, e; Soudijn and Zegers 2012). Therefore, someone who wants to learn can go to a forum. Information is available through the online discussions, and there are also possibilities to pay

people to teach you a specific skill (Hutchings and Holt 2015; Chu et al. 2010; Holt and Lampke 2010). Reliable co-offenders can be found thanks to the rating and review systems on forums (Soudijn and Zegers 2012; Herley and Florencio 2009; Wehinger 2011; Yip et al. 2013; Lusthaus 2012; Dupont et al. 2016; Décary-Hétu and Dupont 2012, 2013; Holt 2013; Holt and Smirnova 2014; Holt et al. 2015; Chu et al. 2010; Ablon et al. 2014).

Local Embeddedness

Little research has been carried out into the local embeddedness of cybercrime (see, among others, Leukfeldt et al. 2017f, 2019; Lusthaus and Varese 2017). Leukfeldt et al. (2017c, d, e) show that phishing and malware attacks on payment transactions are locally embedded. This can be noticed in both Dutch networks and networks operating, for example, from Eastern European countries. Crucial to this type of attack are money mules having accounts to which money can be transferred from victim accounts, before the money is cashed and laundered. When money is transferred to money mules in countries other than that of the victim, this will be noted by the banks using customer payment profiles who monitor and stop unusual transactions. In the next section, criminal money flows will be discussed in greater detail.

Bottlenecks and Criminal Money Flows

The ultimate goal of offenders of financial cybercrime is to make money. However, generating criminal earnings also poses problems for offenders. How can one enjoy ones money without drawing unwanted attention from law enforcement authorities? In other words, managing criminal money flows constitutes a bottleneck in criminal business processes. The following section outlines the earnings, spending, and hiding and laundering of criminal proceeds.

Criminal Earnings

Various estimates of cybercrime markets and the damage caused by cybercrime circulate (e.g., Aldridge and Decary-Hetu (2014; see also EMCDDA 2016), Christin (2012), Holt et al. (2016), Kruithof et al. (2016) (see EMCDDA and Europol 2017), Anderson et al. (2012)). Attempts have also been made to estimate the size of specific online cybercrime markets (e.g., Dhanjani and Rios 2008; Holz et al. 2009), but this seems to be a difficult if not impossible task due to the variety of the offered goods, the lack of clarity about the differences between the asking price and the selling price (the deal being closed outside the forum), and the lack of adequate data or instruments (Holt and Smirnova 2014; Herley and Florencio 2009).

Money flows in traditional organized crime often seem to remain invisible to criminal investigators (Kruisbergen et al. 2016). The same seems to be true for

cybercrime, as research in Sweden and the Netherlands shows (Werner and Korsell 2016; Odinot et al. 2017; Kruisbergen et al. 2018). Nevertheless, several studies do generate important insights into money flows in cybercrime cases. The (presumed) earnings in the 11 Dutch cases Odinot et al. (2017, p. 80) studied ranged from more than 1 million euros to zero or unknown (because no information on earnings was available). Investigation into German cases showed that the "damage" in 18 cases would total 115 million euros (Bulanova-Hristova et al. 2016, p. 207).

Spending Criminal Earnings

When it comes to spending criminal earnings, in terms of both consumption and investments (assets discovered), analyses show neither major differences compared to previous research nor major differences between traditional crime and cybercrime (Kruisbergen et al. 2018). Similar to cases of offline organized crime that have been studied for previous reports of the Dutch Organized Crime Monitor (Kruisbergen et al. 2012, 2015, 2018), for example, some cybercrime cases include offenders who have a lot of money to spend on an expensive lifestyle (Kruisbergen et al. 2018; Odinot et al. 2017, p. 64; Leukfeldt 2014; Leukfeldt et al. 2017c). Earlier research into offline cases of organized crime showed that offenders predominantly invest in their country of origin or in their country of residence, which investments consist of tangible, familiar assets, such as residences, other real estate, and mostly small companies in well-known sectors. In many cases, the available information indicated that the companies in which offenders invest were used for criminal activities, such as transport or money laundering (Kruisbergen et al. 2015). Analyses of the 30 cases in the most recent, fifth data sweep of the Dutch Organized Crime Monitor produce similar results. The 30 cases Kruisbergen and others studied cover traditional types of organized crime as well as cybercrime. Their analyses show no major differences between traditional crime and cybercrime (Kruisbergen et al. 2018).

Hiding and Laundering Criminal Earnings

When it comes to concealing criminal earnings, we do see important differences between traditional organized crime on the one hand and cybercrime on the other (Kruisbergen et al. 2018). Offenders who operate online, similar to their offline counterparts, have to hide their income if they want to prevent detection (and their money seized) by law enforcement. However, in various forms of cybercrime or Internet-facilitated crime, unlike many forms of traditional organized crime, the proceeds are often digital in nature.

This applies, for example, to phishing attacks, banking malware, and ransomware but also to online drug trafficking. Oerlemans et al. (2016) investigated the cash flows associated with banking malware and ransomware. Regarding banking malware, where the damage has been greatly reduced in recent years, use is often made of money mules, people who make their bank account available to criminals

for a fee. Through banking malware, money is initially transferred from the victim's account to an account of a money mule who then withdraws the amount as quickly as possible from an ATM. After cashing (or the cash-out), the money can be transferred to foreign countries, for example, through money transfer offices, after which it is withdrawn again by a (different) money mule abroad. (In addition to money mules, identity fraud can also be used. This means that a payment service is taken via the personal information of a third party. This payment service is then used, for example, to further funnel the received money from the victim.) Another approach is that the money generated through banking malware is used to purchase goods or services directly, such as (luxury) goods at physical or web stores, or bitcoins (Oerlemans et al. 2016). Regarding ransomware, revenues – the ransom – often consist of bitcoins or credits from online vouchers. When bitcoins have been received, the offenders, whether or not they have used a "mixing service," can, for instance, spend or exchange these bitcoins for a cash amount of euros at a physical bitcoin trader or a bitcoin exchange (online exchange service). If the proceeds have been obtained from vouchers purchased by the victim, the value of the vouchers is credited to an online account of an e-wallet service. (An e-wallet is an online payment service (such as PayPal) where money can be put in a personal account, after which payments can be made at web shops (Oerlemans et al. 2016, pp. 107–108).) After which other methods to shield the earning can be applied (Oerlemans et al. 2016).

We will now consider bitcoins, vouchers, and a few other new developments in greater detail. Bitcoin is a cryptocurrency, a decentralized electronic currency. As opposed to regular currencies such as euro or dollar, it is not distributed or controlled by a central bank or any other (centralized) organization. There is, therefore, no formal regulation or supervision governing the use of bitcoin. (This might change as in some countries, such as Japan, where bitcoin is officially regarded as a payment method.) Besides bitcoin there are several other cryptocurrencies, such as Ethereum, Litecoin, and Dogecoin. In terms of market cap, bitcoin has been (and still is) the most important cryptocurrency for quite some time, although the coin's market cap has decreased (EMCDDA 2016) (https://coinmarketcap.com/historical/).

Bitcoins are generated (*mined*) by a decentralized process, through a network of users' computers. The creation of a bitcoin is the result of an algorithm, a mathematical formula. This process requires an enormous computer processing power and consumes a high amount of energy. A person, however, might also simply buy bitcoins using regular currencies, through an online *bitcoin exchange service*. Bitcoins are stored in a *wallet*, a file that is saved on the user's own computer, in the cloud, on a smartphone, or on a USB device (among other things).

Not every type of virtual money or new payment method is operated by decentralized, peer-to-peer technology such as bitcoin. *WebMoney*, for example, is an online payment system which is centrally controlled. It is used for storage and exchange of units of accounts. An account, or *purse*, can be held in several currencies, such as euro, dollar, rubles, and bitcoin. Webmoney is accepted by some webshops (Oerlemans et al. 2016, p. 54) (www.wmtransfer.com).

For people with criminal intentions, bitcoin potentially offers important advantages. As mentioned earlier, bitcoin is not governed by supervision or regulations governing the conventional financial sector, such as the obligation to report a

suspicious transaction. This allows an individual to transfer bitcoins to anyone, anywhere in the world, without having to leave the desk and without having to use a supervised institution. A related advantage concerns the fact that bitcoin transactions offer a certain degree of anonymity (Oerlemans et al. 2016; Kruisbergen and Soudijn 2015).

The unregulated nature and the anonymity of bitcoin, however, have its limitations. For example, buying and selling bitcoins, i.e., exchanging euros for bitcoins and vice versa, takes places through a bitcoin exchange service. In the Netherlands, cryptocurrency exchange services are not subjected to financial regulation. However, larger exchange services have implemented a "know your customer policy" and require identification when a customer turns to them for a transaction. In jurisdictions such as the United States, these exchange services are in fact subjected to supervision (Oerlemans et al. 2016, pp. 108–109). Furthermore, all bitcoin transactions are logged in the *blockchain*. As a result, bitcoin transactions are transparent, since they are publicly available via the blockchain. A bitcoin transaction consists of the transfer of a certain number of bitcoins from one bitcoin address to another, and that is exactly what is recorded in the blockchain. The blockchain, therefore, ensures that a bitcoin can be traced back to its origin. However, the identity of those involved in a bitcoin transaction, i.e., the people behind a sending or receiving bitcoin address, is not revealed in the blockchain. On the other hand, separate transactions may be linked to each other, which might leave, e.g., law enforcement agencies something to work with. Furthermore, individual users of bitcoin technology do not always have the required degree of vigilance and discipline to hide their identity. Meiklejohn et al. (2013) showed that by using network analysis techniques and due to the "unsafe" behavior of users, some bitcoin transactions can in fact be traced back to certain individuals. Particularly where larger amounts of bitcoins are concerned, it could be harder to maintain anonymity (Meiklejohn et al. 2013; Ron and Shamir 2013; Oerlemans et al. 2016; Kruisbergen and Soudijn 2015). Clients may use several services to obscure the traceability of bitcoin transactions (see below).

Besides the fact that anonymity of bitcoin users is not guaranteed, bitcoin also has other drawbacks. Because of the lack of regulation, bitcoin users are not protected by the safeguards applied to the formal financial sector. As a result, users are vulnerable for losses caused by fraud, bankruptcy, and other misfortune. Customers of the once very popular bitcoin exchange service Mt. Gox, for example, suffered when hundreds of thousands of bitcoins "disappeared" in 2014. (Moore and Christin (2013) discuss the risks involved in the use of bitcoin exchange services (their chapter was published before the disappearance of bitcoins at Mt. Gox came to light).) Furthermore, hackers stole large amounts of the cryptocurrency Ethereum in 2017. (https://www.cnbc.com/2017/07/17/coindash-website-hacked-7-million-stolen-in-ico.html.) Another risk concerns the very volatile currency exchange rate. Finally, the acceptance of bitcoin as a payment method in the regular economy is still limited, although the level of acceptance is increasing (Kruisbergen and Soudijn 2015; Oerlemans et al. 2016).

The most striking continuity in money laundering methods as well as the most striking similarity between cybercrime and traditional crime is the preference of offenders for cash. "Traditional" organized crime offenders, i.e., offenders

participating in offline types of organized crime, as well as cybercrime offenders, prefer cash (Kruisbergen et al. 2018; Soudijn 2017, 2018; Europol 2015). Cybercrime offenders often change their digital currencies for cash, at least in part. (This process is probably also one of the most important bottlenecks in these types of criminal operations, because changing digital currencies for cash in many cases produces some sort of trace or paper trail.) In cases of phishing attacks, banking malware, and ransomware, revenues, after using money mules or exchanging services, often end up as "hard cash" in the hands of the main offenders. Likewise, online drug traffickers seem to exchange the bitcoins they receive for cash (Leukfeldt 2014; Leukfeldt et al. 2017a, b, c; Odinot et al. 2017, p. 38; Oerlemans et al. 2016; Kruisbergen et al. 2018). The use of new payment methods, such as cryptocurrencies and prepaid cards, offers new possibilities for offenders, but in practice they are predominantly used in combination with cash. Europol speaks of a *symbiosis* of traditional methods and new technology (Europol 2015). The importance of cash for the criminal economy might even have increased, due to the fact that digital payment methods often produce traces and because of strict regulation of the legal financial sector (Europol 2015; Soudijn 2017, 2018).

The moment a cybercrime offender holds his criminal earnings in cash, he may use the same methods to conceal his money as offenders in other types of crime do. The criminal money can be transferred (physically or by using money transfer services or underground banking), cash might be used to buy valuable goods (whether or not through using straw men or other schemes), and the money might be laundered, for example, by faking legal economic activities (Kruisbergen et al. 2018; Europol 2015, pp. 370–378).

To conceal criminal earnings, offenders in cybercrime cases may use several (new) types of service providers who, willingly or unwillingly, become involved in criminal money flows. Some private bitcoin exchangers, for example, can be considered as professional facilitators who willingly provide essential financial services to offenders. For obvious reasons, cybercrime offenders do not want to use a regular bitcoin exchange company to exchange their bitcoins (since regular exchange services often require identification). Offenders instead rely on private bitcoin exchangers who specialize in discrete financial service. These exchangers receive a relatively high commission to exchange the illegally earned bitcoins for cash euros (Kruisbergen et al. 2018).

So-called *e-wallet* services play a crucial role in the process of purchasing and selling bitcoins. These services offer the possibility of obscuring the link between a bitcoin address from which a bitcoin has been sent and a receiving address. Besides specialized e-wallets, several services are available on the Internet to diminish the traceability of bitcoins, so-called mixing or tumbler services, such as *bitcoin fog* and *helix*. Other service providers that might be used concern, the earlier mentioned, *payment service providers* and providers of *prepaid cards*. Furthermore, specific types of straw men, *money mules*, are often used in cases of banking malware and phishing. Analyses of Oerlemans and others show that these mules are predominantly recruited from young adults (18–22 years old) in disadvantaged areas in big cities (Oerlemans et al. 2016; see also Maurtiz 2014). Finally, *banks* are crucial,

since banks provide the infrastructure that banking malware offenders and bitcoin exchangers, for example, take advantage of. Due to several measures taken by banks, the financial damage as a result of banking malware has decreased enormously recently (EMCDDA 2016; Odinot et al. 2017; Oerlemans et al. 2016; Soudijn 2017; Nederlandse Vereniging van Banken (NVB) 2017).

Conclusion

IT clearly has an impact on criminal collaborations: it offers offenders new possibilities in the area of criminal cooperation, with regard to logistical aspects of the criminal business process and with regard to criminal money flows. This way, IT shifts the horizon for offenders looking for victims, co-offenders, tools, or customers. Due to the Internet, offenders who wish to steal money from victims are able to throw out a large dragnet. Offenders seeking specific knowledge or tools can find these through criminal meeting places on the Internet. IT thus leads to new forms of cooperation. Furthermore, both suppliers and consumers of drugs find market places on the dark web that are, in essence, free of physical and social limitations. Contacts in the offline world and close social relationships to this extent seem less important because it is easier to find people, expertise, and tools. Trust, for example, in the expertise of possible co-offenders or between buyers and sellers is, however, still essential. Trust is now being established using the opportunities the Internet offers to check the reputation of others (Holt et al. 2015; Décary-Hétu and Dupont 2013; et al. 2016; Soudijn and Monsma 2012).

Offenders also make use of opportunities to communicate with each other in a protected manner. Technological developments have made encrypted communication accessible to everyone. Hardware and software for shielded communication are easily obtained and offer an important advantage to offenders wishing to coordinate business without police interception. Furthermore, IT facilities, such as cryptocurrencies, are also an important innovation. Cryptocurrencies have a certain degree of anonymity and are the means of payment on dark net markets. Together with TOR networks on which dark net markets operate, a currency such as bitcoin makes it possible for buyers and sellers of illegal goods and services to enter into more or less anonymous transactions.

These new possibilities offered by IT have implications for the ways offenders operate. Looking at cybercrime cases, interesting parallels could be drawn with more traditional organized crime. For example, it can be noticed that cybercrime cases are, to a certain extent, locally embedded (see also Leukfeldt et al. 2017b, c, d, 2019; Lusthaus and Varese 2017; Kruisbergen et al. 2018). Some of the main offenders in cybercrime cases seem to share the same physical environment (because they know each other, e.g., from the neighborhood or nightlife), and money mules are often found in the immediate social vicinity. The sources of social capital that are used for getting involved in organized forms of cybercrime, therefore, also consist largely of offline and local interactions.

Despite the fact that online marketplaces are theoretically not hindered by borders, dark net markets also seem to have an important local (regional) physical component. For example, important sellers on the online marketplace studied by Kruisbergen et al. (2018) and Kruithof et al. (2016) handled their transactions, particularly those of larger sizes, through physical meetings. Furthermore, in a large part of the transactions done on the marketplace, buyer and seller appeared to live in nearby countries. It is possible that the offenders think that, currently, sending postal items is too risky.

Finally, some offenders still depend on local facilities, such as postal companies for online drug vendors and public places with Wi-Fi access (such as fast-food restaurants) for bitcoin exchangers. Another important finding is that cybercriminals still seem to prefer cash. For traditional forms of organized crime, the dominance of cash is a known fact, but also offenders operating online seem to have a preference to exchange at least part of their digital revenue for cash.

Cross-References

- ▶ Computer Hacking and the Hacker Subculture
- ▶ Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective
- ▶ Data Breaches and Carding
- ▶ Deviant Instruction: The Applicability of Social Learning Theory to Understanding Cybercrime
- ▶ Financial Crimes: How New Technology Changes the Game
- ▶ Identity Theft: Nature, Extent, and Global Response
- ▶ Organized Crime and Cybercrime
- ▶ Organized Financial Cybercrime: Criminal Cooperation, Logistic Bottlenecks and Money Flows
- ▶ Phishing and Financial Manipulation
- ▶ Police and Extralegal Structures to Combat Cybercrime
- ▶ Rational Choice/Deterrence
- ▶ Routine Activities
- ▶ Social Engineering
- ▶ Spam-Based Scams
- ▶ The Dark Web and its Affordances: An Exploration of Illicit Drug, Firearm, Sex, and Cybercrime Markets

References

Ablon, L., Libicki, M.C., & Golay, A.A. (2014). *Markets for cybercrime tools and stolen data. Hackers' Bazaar.* RAND: www.rand.org

Aldridge, J., & Décary-Hétu, D. (2014). *Not an 'eBay for drugs': The cryptomarket 'Silk Road' as a paradigm shifting criminal innovation*. http://ssrn.com/abstract=2436643, geraadpleegd April 2018.

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., & Moore, T. (2012). *Measuring the cost of cybercrime*. Presented at the Workshop on the Economics of Information Security (WEIS), Berlin, Germany. Retrieved from https://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Andresen, M. A., & Felson, M. (2010). Situational crime prevention and co-offending. *Crime Patterns and Analysis, 3*(1), 3–13.

Bijlenga, N., & Kleemans, E. R. (2018). Criminals seeking ICT-expertise: An exploratory study of Dutch cases. *European Journal of Criminal Policy and research*. https://doi.org/10.1007/s10610-017-9356-z.

Bouchard, M., & Morselli, C. (2014). Opportunistic structures of organized crime. In L. Paoli (Ed.), *The Oxford handbook of organized crime*. Oxford/New York: Oxford University Press.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). *Organization and cyber crime*: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology, 8*(1), 1–20.

Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M., Pool, R., Poot, C. de, Werner, W., & Korsell, L. (Eds.) (2016). Cyber-OC - Scope and manifestations in selected EU member states. Wiesbaden: Bundeskriminalamt.

Christin, N. (2012). *Traveling the silk road: A measurement analysis of a large anonymous online marketplace*. Pittsburgh: Carnegie Mellon University.

Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examining the creation, distribution, and function of malware on-line.* Technical Report for National Institute of Justice. NIJ Grant No. 2007-IJ-CX-0018. Available at https://www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime, 13*(3), 160–175.

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime, 14*(2–3), 175–196.

Décary-Hétu, D., Morselli, C., & Leman-Langlois, S. (2012). Welcome to the scene: A study of social organization and recognition among warez hackers. *Journal of Research in Crime and Delinquency, 49*(3), 359–382.

Dhanjani, N., & Rios, B. (2008). *Bad sushi: Beating phishers at their own game*. Paper presented at the Annual Blackhat Meetings. Las Vegas.

Dupont, B., Côté, A. M., Savine, C., & Décary Hétu, D. (2016). The ecology of trust among hackers. *Global Crime, 17*(2), 129–151.

Dupont, B., Côté, A. M., Boutin, J. L., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of "the Most Dangerous Cybercrime Forum in the World". *American Behavioral Scientist*. https://doi.org/10.1177/0002764217734263.

Edwards, A., & Levi, M. (2008). Researching the organization of serious crimes. *Criminology and Criminal Justice, 8*(4), 363–388.

EMCDDA (European Monitoring Centre for Drugs and Drug Addiction). (2016). *The internet and drug markets*. Luxemburg: Publications Office of the European Union.

EMCDDA (European Monitoring Centre for Drugs and Drug Addiction) & Europol. (2017). *Drugs and the darknet: Perspectives for enforcement, research and policy.* Luxemburg: Publications Office of the European Union.

European Police Office (Europol) (2015). Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering. *Trends in Organized Crime*, 18: 355–379.

Felson, M. (2003). The process of co-offending. In M. J. Smith & D. B. Cornish (Eds.), *Theory for practice in situational crime prevention* (Vol. 16, pp. 149–168). Devon: Willan Publishing.

Felson, M. (2006). *The ecosystem for organized crime* (HEUNI paper nr 26). Helsinki: HEUNI.

Franklin, J., Paxson, V., Perrig, A., Savage, S. (2007). *An inquiry into the nature and cause of the wealth of internet miscreants*. Paper presented at *CCS07*, October 29–November 2, 2007 in Alexandria.

Grabosky, P. (2007). The internet, technology, and organized crime. *Asian Criminology, 2*(2), 145–161.

Herley, C., & Florencio, F. (2009). *Nobody sells gold for the price of silver: Dis-honesty, uncertainty and the underground economy*. Redmond: Microsoft. Microsoft TechReport nr. MSR-TR-2009-34.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*(2), 171–198.

Holt, T. J. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime, 14*(2–3), 155–174.

Holt, T. J., & Kilger, M. (2008). Techcrafters and makecrafters: A comparison of two populations of hackers. *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing, 67–78.*

Holt, J. T., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*(1), 33–50.

Holt, T. J., & Smirnova, O. (2014). *Examining the structure, organization, and processes of the international market for stolen data*. Washington, DC: U.S. Department of Justice.

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Crimi-nology (IJCC), 6*(1), 891–903.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime, 16*(2), 81–103.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior, 37*(4), 353–367. https://doi.org/10.1080/01639625.2015.1026766.

Holz, T., Engelberth, M., & Freiling, F. (2009). Learning more about the under-ground economy: A case-study of keyloggers and dropzones. In M. Backes & P. Ning (Eds.), *Computer security-ESCORICS* (pp. 1–18). Berlin/Heidelberg: Springer.

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change, 62*(1), 1–20.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology, 55*(3), 596–614.

Ianni, F. A. J., & Reuss-Ianni, E. (1972). *A family business; kinship and social control in organized crime*. London: Routledge & Kegan Paul.

Kleemans, E. R., & De Poot, C. J. (2008). Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology, 5*(1), 69–98.

Kruisbergen, E. W., & Soudijn, M. R. J. (2015). Wat is witwassen eigenlijk? Introductie tot theorie en praktijk. *Justitiële verkenningen, 41*(1), 10–23.

Kruisbergen, E. W., Van de Bunt, H. G., & Kleemans, E. R. (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit [Organized crime in the Netherlands. Fourth report of the Organized Crime Monitor]*. Den Haag: Boom Lemma. English summary available at: https://english.wodc.nl/.

Kruisbergen, E. W., Kleemans, E. R., & Kouwenberg, R. F. (2015). Profitability, power, or proximity? Organized crime offenders investing their money in legal economy. *European Journal on Criminal Policy and Research, 21*(2), 237–256.

Kruisbergen, E. W., Kleemans, E. R., & Kouwenberg, R. F. (2016). Explaining attrition: Investigating and confiscating the profits of organized crime. *European Journal of Criminology*. https://doi.org/10.1177/1477370816633262.

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2018). *Georganiseerde criminaliteit en ICT Nederland. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit [Organized crime and IT. Report based on the fifth round of the Organized Crime Monitor]*. Den Haag: WODC. English summary available at: https://english.wodc.nl/.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*. Santa Monica/Cambridge: Rand Corporation.

Leukfeldt, E. R. (2014). Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime, 17*(4), 231–249.

Leukfeldt, E. R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Den Haag: Eleven International Publishers.

Leukfeldt, E. R. (2017). *Research agenda the human factor in cybercrime and cybersecurity*. Den Haag: Eleven International Publishing.

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017a). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research, 23*(3), 287–300.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). A typology of cybercriminal networks: From low tech locals to high tech specialists. *Crime, Law and Social Change*. https://doi.org/10.1007/s10611-016-9646-2.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017c). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*. https://doi.org/10.1093/bjc/azw009.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017d). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*. https://doi.org/10.1007/s10611-016-9647-1.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017e). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist*. https://doi.org/10.1177/0002764217734267.

Leukfeldt, E. R., de Poot, C., Verhoeven, M., Kleemans, E. R., & Lavorgna, A. (2017f). Cyber-criminal networks. In E. R. Leukfeldt (Ed.), *Research agenda: The human factor in cybercrime and cybersecurity*. Den Haag: Eleven International Publishers.

Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. (2019). Criminal networks in a digitized world: On the Nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-019-09366-7.

Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social network analysis of a criminal hacker community. *Journal of Computer Information Systems, 51*(2), 31–41.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime, 13*(2), 71–94.

Lusthaus, J., & Varese, F. (2017). Offline and local; the hidden face of cybercrime. *Policing: A Journal of Policy and Practice*. https://doi.org/10.1093/police/pax042.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). *A fistful of bitcoins: Characterizing payments among men with no names*. San Diego: University of California. Geraadpleegd April 2018. https://doi.org/10.1145/2504730.2504747.

Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of bit-coin-exchange risk. In A. R. Sadeghi (Ed.), *Financial cryptography and data security, FC 2013, lecture notes in computer science* (Vol. 7859). Berlin: Springer.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2013). An analysis of underground forums. *IMC'11* 71–79.

Maurtiz, H. (2014). De aard en omvang van Money Muling: Fraude met internetbankieren en witwassen. [Money Muling] Scriptie, uitgevoerd voor de Nationale Politie.

NVB (Nederlandse Vereniging van Banken). (2017). *Factsheet Veiligheid en fraude*. Z. pl.:NVB. www.nvb.nl

Odinot, G., Verhoeven, M. A., Pool, R. L. D., & De Poot, C. J. (2017). *Organised cyber-crime in the Netherlands: Empirical findings and implications for law enforcement*. Den Haag: WODC. Cahier 2017-1.

Oerlemans, J. J., Custers, B. H. M., Pool, R. L. D., & Cornelisse, R. (2016). *Cybercrime en witwassen: Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*. Den Haag: Boom criminlogie. Onderzoek en beleid 319.

Peretti, K. K. (2008). Data breaches: What the underground world of 'carding' reveals. *Santa Clara Computer and High-technology Law Journal, 25*(2), 345–414.

Reiss, A. J. (1988). Co-offending and criminal careers. In M. Tonry & N. Morris (Eds.), *Crime and justice. A review of research*. Chicago: Chicago University Press.

Reiss, A. J., & Farrington, D. P. (1991). Advancing knowledge about co-offending: Results from a prospective longitudinal survey of London males. *Journal of Criminal Law and Criminology, 82*(2), 360–395.

Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. *Financial Cryptography and Data Security, 7859*, 6–24.

Shaw, C. R., & McKay, H. D. (1931). *Report on the causes of crime: Volume II*. Washington, DC: Government Printing Office.

Soudijn, M. R. J. (2017). *Witwassen: Criminaliteitsbeeldanalyse 2016* (Crime Pattern Analyses on Money Laundering). Driebergen: Landelijke Eenheid.

Soudijn, M. R. J. (2018). Using police reports to monitor money laundering developments. Continuity and change in 12 years of dutch money laundering crime pattern analyses. *European Journal of Criminal Policy and Research*. https://doi.org/10.1007/s10610-018-9379-0.

Soudijn, M. R. J., & Monsma, E. (2012). Virtuele ontmoetingsuimtes voor cybercrimi-nelen. *Tijdschrift voor Criminologie, 54*(4), 349–360.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime, 15*(2–3), 111–129.

Sutherland, E. H. (1937). *The professional thief*. Chicago: The University of Chicago Press.

Wehinger, F. (2011). The dark net: Self-regulation dynamics of illegal online markets for identities and related services. *Intelligence and Security Informatics Conference*. https://doi.org/10.1109/EISIC.2011.54.

Werner, Y., & Korsell, L. (2016). Cyber-OC in Sweden. In G. Bulanova-Hristova, K. Kasper, G. Odinot, M. Verhoeven, R. Pool, C. de Poot, W. Werner, & L. Korsell (Eds.), *Cyber-OC: Scope and manifestations in selected EU member states* (pp. 101–164). Wiesbaden: Bundeskriminalamt.

Yip, M., Shadbolt, N., & Webber, C. (2012). Structural analysis of online criminal social networks. In *IEEE international conference on intelligence and security informatics (ISI)* (pp. 60–65). Arlington: IEEE.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society, 23*(4), 516–539.